GIBBS LAW GROUP LLP
David Berger (State Bar No. 277526)
Jane Farrell (State Bar No. 333779)
Sarah E. Hillier (*pro hac vice* forthcoming)
Jennifer Sun (State Bar No. 354276)
1111 Broadway, Ste. 2100
Oakland, CA 94607
Tel: 510-350-9700
dmb@classlawgroup.com
jgf@classlawgroup.com
seh@classlawgroup.com
jsun@classlawgroup.com

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF CALIFORNIA
SACRAMENTO DIVISION

EVAN GRAMELSPACHER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

POWERSCHOOL HOLDINGS, INC. and POWERSCHOOL GROUP LLC,
Defendants.

Case No. _____

CLASS ACTION COMPLAINT FOR:

1. NEGLIGENCE
2. NEGLIGENCE PER SE
3. BREACH OF THIRD-PARTY BENEFICIARY CONTRACT

JURY TRIAL DEMANDED

COMPLAINT – CLASS ACTION

Plaintiff Evan Gramelspacher ("Plaintiff"), individually and on behalf of the proposed class defined below, bring this class action against Defendants PowerSchool Holdings, Inc. and PowerSchool Group LLC (collectively, "Defendants" or "PowerSchool") and alleges the following:

NATURE OF THE ACTION

1. PowerSchool is the nation's largest provider of cloud-based education technology software. PowerSchool's products are primarily used by school districts and educators to store and update records on students in grades K-12. PowerSchool software is used to support tens of millions of students—approximately 75 percent of K-12 students in North America. As part of its business, PowerSchool processes and stores personally identifying information ("PII") and/or protected health information ("PHI") of teachers and, students, and their guardians.

2. Despite holding the highly sensitive personal information of tens of millions of people—most of whom are minors—PowerSchool left gaping cybersecurity holes. Unbeknownst to its customers or end users, PowerSchool stored PII and PHI (collectively, "Private Information") in either unencrypted or inadequately encrypted formats on an Internet-accessible environment, that did not support multi-factor authentication and allowed the hackers to access and then exfiltrate vast amounts of data from that website.

3. At some point between December 19 and December 28, 2024, hackers breached the company's vulnerable systems and exfiltrated the valuable Private Information stored within (the "Data Breach"). PowerSchool failed to detect the hackers' actions until the hacker contacted them on December 28, 2024. Beginning on January 8, 2025, PowerSchool began notifying customers that their data was accessed and that they were impacted.

4. Now, Plaintiff Gramelspacher and other members of the proposed class must deal with the fallout. According to public reports, the hacker claimed to have taken data on 62,488,628

students and 9,506,624 teachers in North America.[1] PowerSchool has neither confirmed nor denied the accuracy of these numbers, nor has it identified the precise number of these victims that reside in the United States.

5. The Private Information stolen in the Data Breach includes dates of birth, addresses, phone numbers, emails, photo identification, and tax information numbers. The hackers obtained Social Security numbers for roughly 25% of the class, putting them at risk for a vast array of identity theft and fraud for years to come. The hackers further obtained an unknown number of victims' health histories and other medical information. Plaintiff's information continues to reside on or remain accessible through PowerSchool's systems.

6. Plaintiff Gramelspacher by this action seeks compensatory damages as well as injunctive relief to remediate PowerSchool's deficient cybersecurity and provide credit monitoring, identity theft insurance, and credit repair services (or the money needed to secure those services) to protect him and the other breach victims from identity theft and fraud.

7. This Data Breach directly resulted from PowerSchool's failure to implement reasonable and adequate cybersecurity controls to protect the Private Information entrusted to it from a foreseeable and preventable cyberattack.

8. After numerous high-profile cyberattacks across all industries in recent years and numerous warnings by government agencies, such a data breach was a known risk to PowerSchool. Still, PowerSchool failed to take the necessary steps to secure Private Information.

9. With the Private Information accessed in the Data Breach, data thieves could potentially commit various crimes in the future, such as selling Class members' Private Information on the Dark Web, opening new financial accounts in Class members' names, obtaining loans in Class members' names, using their information to access government benefits, filing fraudulent tax returns, obtaining driver's licenses with Class members' names but another person's photograph, and providing false information to law enforcement during an arrest.

[1] Lawrence Abrams, *PowerSchool hacker claims they stole data of 62 million students*, BleepingComputer, January 22, 2025, https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/.

10. As a result of the Data Breach, Plaintiff and Class members suffered concrete injuries-in-fact including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains inadequately secured and available for unauthorized third parties to access and abuse; and (b) remains in PowerSchool's possession and is subject to further unauthorized disclosures so long as PowerSchool fails to undertake appropriate and adequate measures to protect the Private Information.

11. Plaintiff initiates this class action lawsuit on behalf of all those similarly situated to address PowerSchool's inadequate safeguarding of Class members' Private Information, which it collected and maintained.

PARTIES

12. Plaintiff Evan Gramelspacher is eighteen years old and is a student in the Olentangy Local School District, which is based in Lewis Center, Ohio. At all relevant times, he has been domiciled in and a citizen of the state of Ohio. PowerSchool obtained and stored Mr. Gramelspacher's Private Information in connection with his schooling in the Olentangy Local School District.

13. Defendant PowerSchool Holdings, Inc., is a Delaware corporation with its principal place of business at 150 Parkshore Dr., Folsom, California 95630.

14. Defendant PowerSchool Group LLC is a Delaware Limited Liability Company with its principal place of business at 150 Parkshore Dr., Folsom, California 95630.

15. At all relevant times, each Defendant was a principal, agent, alter ego, joint venturer, partner, or affiliate of each other, and in doing the acts alleged herein, was acting within the course and scope of that principal, agent, alter ego, joint venture, partnership, or affiliate relationship. Each Defendant had actual knowledge of the wrongful act of each other; ratified,

approved, joined in, acquiesced, or authorized the wrongful acts of each other; and retained the benefits of those wrongful acts.

JURISDICTION AND VENUE

16. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative Class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiff is (and many members of the proposed Class are) a citizen of a state different from Defendants.

17. This Court has personal jurisdiction over Defendants because they are headquartered in and have their principal place of business in this District. Defendants conduct substantial business and have minimum contacts with the State of California.

18. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants are headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

PowerSchool's Business

19. PowerSchool holds itself out "[a]s a leading provider of cloud-based software in North America." Its products support vast numbers of teachers, students, and their parents. PowerSchool holds the Private Information of 75 percent of North American students. Over 18,000 customers rely on PowerSchool, including 90 of the largest 100 districts by student enrollment.

20. PowerSchool built itself into a market leader in education technology. It was so successful that in 2024, it was purchased by private investment firm, Bain Capital, for $5.6 billion.

21. The data PowerSchool collects far exceeds traditional education records of school-age children, including thousands of person-specific data fields.

22. PowerSchool collects and maintains the Private Information of customers and end-users, including:

Name
Residential address
Phone number

Email address
Date of birth
Demographic information
Social Security number
Tax identification number
Financial information
Medication information
Disability information
Health insurance information
Photo identification
Employment information

23. Indeed, the stolen data even included personal information regarding parental access rights to children, parental restraining orders, and instructions about when certain students need to take medication.[2]

The Data Breach

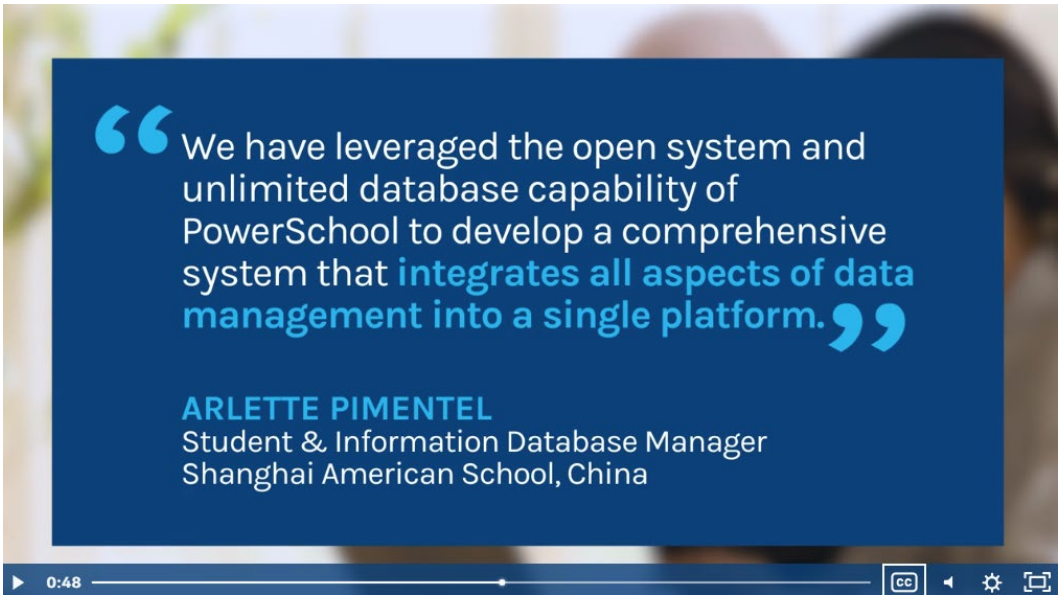
24. As of this writing, PowerSchool has provided scant information about what happened in the data breach – but the available information shows serious gaps in PowerSchool's information security controls.

25. On December 19, 2024, financially-motivated hackers were able to use compromised credentials to access PowerSource, a "community-focused customer portal."[3] When used appropriately, PowerSource "is available to all district and school staff, including teachers, administrators and IT staff."[4] PowerSchool has admitted that at the time of the data breach, PowerSource did not support (let alone require) multi-factor authentication, a standard information security control that *on its own* would have prevented this Data Breach.[5]

[2] Carly Page, What PowerSchool isn't saying about its 'massive' student data breach, TechCrunch, Jan. 22, 2025, https://techcrunch.com/2025/01/22/what-powerschool-isnt-saying-about-its-massive-student-data-breach/.
[3] *Id.* (quoting PowerSchool spokesperson Beth Keebler).
[4] PowerSource, *Welcome to PowerSource*, https://support.powerschool.com/login.action?redirect=http%3A%2F%2Fsupport.powerschool.com%2Fhome%2Fmain.action (last visited January 22, 2025).
[5] Page, *supra* note 2.

26. The hackers then spent the next couple of weeks conducting reconnaissance in the PowerSchool environment.[6] Failing to notice active hacking over weeks indicates that PowerSchool either lacked standard intrusion detection systems adequate to notice this suspicious activity or that PowerSchool personnel failed to heed the warning of their systems. If PowerSchool had properly implemented and configured these standard information security controls, this Data Breach would not have happened or would have been halted before the data was exfiltrated.

27. Moreover, PowerSource was configured to allow users to access the vast array of data that PowerSchool stored in its PowerSchool SIS system. PowerSchool's marketing emphasizes that their Student Information System ("SIS") operates as, essentially, a one-stop shop for *all* student data. The marketing materials for PowerSchool SIS describe it as "one secure customizable platform providing the interoperability needed to power your school and district operations with accurate student data."[7]



[6] Andy Lombardo, The PowerSchool Data Breach: What we know today, how to check your exposure, and how to see what fields were exfiltrated, EDTECHIRL.COM, Jan. 9, 2025, https://www.edtechirl.com/p/the-powerschool-data-breach-what.

[7] "PowerSchool SIS at-a-glance," video found at https://www.powerschool.com/student-information-cloud/powerschool-sis/ (last visited January 21, 2025).

28. PowerSchool SIS gathers data on students and families directly from students and their families as it provides the platform families use for online enrollment in its customers' schools and districts.[8]

29. PowerSchool SIS also gathers data on students and families from its customers and their employees, including data on "attendance, behavior, health, graduation tracking, asset tracking, and student demographics."[9]

30. From a cybersecurity perspective, it is inexcusable that a company would allow access to such sensitive information through an internet-facing portal that is not protected by multi-factor authentication. But PowerSchool's security failings are far worse than just this.

31. Typically, when hackers are able to use stolen credentials, they are able to get access to whatever data the rightful owner of those credentials would be permitted to see. Here, however, the hackers were able to access the collective data of thousands of different users. This indicates either that PowerSchool's systems were internally misconfigured to permit dangerously broad access or that PowerSchool failed to prevent the theft of high-level administrative credentials, which should have required multiple security controls to use.

32. On December 22, the hackers were able to use a data export tool normally used for remote support to create and export two massive data files: students_export.csv and teachers_export.csv.[10] Once again, standard information security controls should have prevented

[8] "*Id.*; "Explore All PowerSchool SIS Has to Offer," https://www.powerschool.com/student-information-cloud/powerschool-sis/features/ (last visited January 21, 2025).
[9] "School Operations and Compliance," https://www.powerschool.com/student-information-cloud/powerschool-sis/ (last visited January 21, 2025).
[10] Lombardo, *supra* note 6.

this activity. For example, PowerSchool should have implemented Data Loss Prevention (DLP) technology that would have noticed this data aggregation, particularly from so many different customers, and halted the action. A DLP solution also would have integrated with PowerSource's intrusion detection systems to immediately alert information security personnel to the hackers' presence. Again, these are standard information security controls that any entity hosting massive quantities of Private Information should have implemented.

33. In fact, PowerSchool's security was so poor that it allowed the hackers to obtain data from PowerSchool customers that hosted their own data on their own servers around the country.[11] As long as they were using PowerSchool SIS, they were vulnerable.

34. Once the hackers had aggregated millions of records into these two files, they exfiltrated the data without PowerSchool ever noticing such massive data transfers. Again, properly implemented intrusion detection and DLP tools would have stopped the hackers from obtaining the data files. But PowerSchool's information security controls again failed.

35. PowerSchool never even learned of the Data Breach until December 28, 2024, when the hackers contacted PowerSchool to seek a ransom in exchange for purportedly deleting the data.

36. PowerSchool investigated the Data Breach and identified the compromised products and customers. It confirmed that the breach affected "families and educators" and various types of sensitive Private Information, including "the individual's name, contact information, date of birth, limited medical alert information, Social Security Number (SSN), and other related information."[12]

37. On January 8, 2025, it publicly announced the Data Breach and began notifying customers.

[11] *Id.*

[12] PowerSchool, SIS Incident landing page, https://www.powerschool.com/security/sis-incident/ (last visited January 22, 2025)

PowerSchool's Data Security Representations

38. PowerSchool knew its obligations in ensuring data security and understood the importance of "safe collection and management of student data."[13]

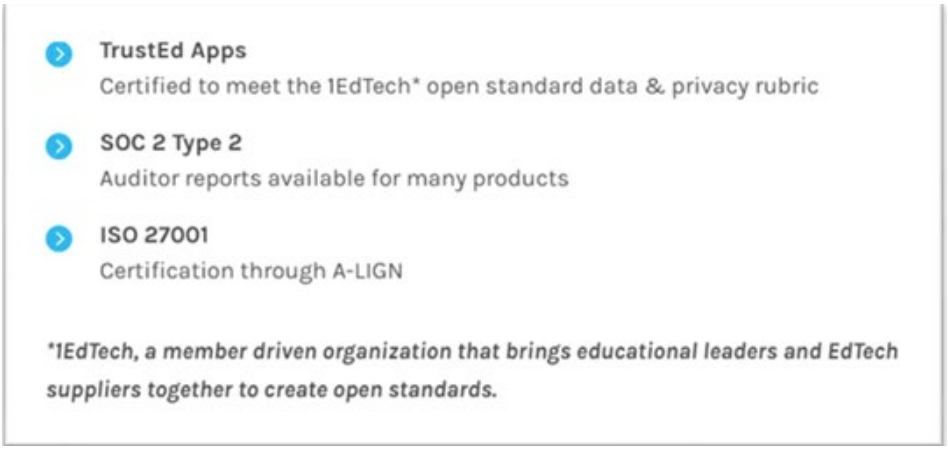
39. For example, the marketing video with which PowerSchool advertises PowerSchool SIS includes an emphasis on the security of PowerSchool SIS[14]:

40. PowerSchool has multiple webpages dedicated to its privacy and security capabilities. It represents that it uses "industry standards" to "improve data integrity and

[13] PowerSchool, *Top 6 Best Practices for Improving Student Information System (SIS) Cybersecurity*, Sept. 10, 2024, https://www.powerschool.com/blog/best-practices-improving-sis-cybersecurity/.

[14] "PowerSchool SIS at-a-glance," video found at https://www.powerschool.com/student-information-cloud/powerschool-sis/ (last visited January 21, 2025).

security."[15] It claims that all products are "[c]ertified to meet the 1EdTech open standard data & privacy rubric," and have received "ISO 27001" certification through "A-LIGN."



41. The top line of its "Cybersecurity, Data Privacy, and Infrastructure" webpages states that "PowerSchool is committed to being a good custodian of student data, taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability."[16]

42. In its privacy policy, PowerSchool boasts that it "places great importance and value on the proper handling of personal data that flows within our product as we provide services to our customers."[17] To this end, PowerSchool claims that it has the "relevant security and privacy policies to drive expectations from the workforce":

> We seek to protect our customers' personal data from unauthorized access, use, modification, disclosure, loss, or theft by leveraging various reasonable security measures and methods to secure our customers' personal data throughout its processing lifecycle with PowerSchool applications. Our overall aim is to ensure the confidentiality, integrity, and availability of our customers' personal data by leveraging technical, organizational, and where appropriate, physical security methods. Security protection at PowerSchool is a cross-functional activity that intersects our workforce duties, and we have relevant security and privacy policies to drive expectations from the workforce.[18]

[15] PowerSchool, *Interoperability Overview*, https://www.powerschool.com/interoperability-overview/ (last visited January 22, 2025).
[16] "PowerSchool's Privacy Principles," PowerSchool, https://www.powerschool.com/privacy/ (last visited January 21, 2025).
[17] *Id.*
[18] *Id.*

43. Under "Frequently Asked Questions," PowerSchool represents that it protects data by using "state-of-the-art, and appropriate physical, technical, and administrative security measures to protect the personal data that we process."[19]

44. PowerSchool's Global Privacy Statement, last updated October 1, 2024, makes the following representations about PowerSchool's data security measures:

> Whether PowerSchool is a collector or processor or your data, PowerSchool is committed to protecting your personal information. PowerSchool uses commercially reasonable physical, administrative, and technical safeguards to preserve the confidentiality, integrity, and availability of your personal information. Our systems are regularly certified by third parties against industry security standards from AIPCA and ISO. As customers provide PowerSchool with Customer Data to process, PowerSchool makes commercially reasonable efforts to ensure the security of our systems. Please note that this is not a guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, administrative, and technical safeguards.
>
> …
>
> PowerSchool employs a variety of physical, administrative, and technological safeguards designed to protect your data against loss, misuse, and unauthorized access or disclosure. We strive to continuously maintain reasonable physical, administrative, and technical security measures. Our security measures consider the type and sensitivity of the data being collected, used, and stored, and the current state of technology and threats to data. PowerSchool independently verifies its security management system to the internationally recognized standard for security management and holds ISO 27001 and SOC2 certifications. PowerSchool also endeavors to align its privacy and security operations to best practices and relevant international regulations.[20]

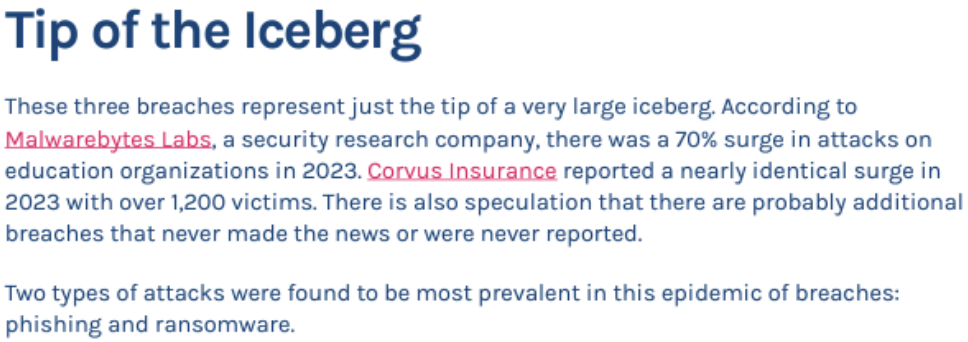
45. In "PowerSchool: A Leader in Responsible AI for Education," a PDF linked on its website, PowerSchool states: "As the education sector has become more reliant on digital technologies, we face increasing cybersecurity threats from hackers who seek to exploit vulnerabilities, steal data, or disrupt operations." PowerSchool mentions 3 school cybersecurity attacks that occurred in 2023 and notes that these are "just the tip of a very large iceberg."[21]

---

[19] *Id.*

[20] *Id.*

[21] "PowerSchool: A Leader in Responsible AI for Education," June 10, 2024, https://go.powerschool.com/rs/861-RMI-



Tip of the Iceberg

These three breaches represent just the tip of a very large iceberg. According to Malwarebytes Labs, a security research company, there was a 70% surge in attacks on education organizations in 2023. Corvus Insurance reported a nearly identical surge in 2023 with over 1,200 victims. There is also speculation that there are probably additional breaches that never made the news or were never reported.

Two types of attacks were found to be most prevalent in this epidemic of breaches: phishing and ransomware.

46. In a section of the PDF discussing ransomware threats, PowerSchool specifically advises readers to not pay a ransom or negotiate with hackers because "[p]aying the ransom does not guarantee that you will get your data back, or that it will not be leaked or sold. It also … makes you a more attractive target for future attacks."[22]

Plaintiff's Private Information Has Value

47. Criminal actors covet PHI and PII, which allow criminals to conduct an immense array of crimes that harm the data subjects. Such information is continually traded through illicit criminal networks and on underground "dark web" marketplaces that cannot be accessed through standard web browsers.

48. Private Information can be sold at a price ranging from $40 to $200.[23]

49. The kind of information exposed in the Data Breach is of much higher value than simple credit card information, for which customers can change or close accounts.[24] Much of the PII exposed in the Data Breach is immutable and cannot readily be changed—*e.g.*, date of birth, addresses and Social Security numbers.

846/images/Responsible_AI_Cybersecurity_Report.pdf?version=0 (last visited January 22, 2025).

[22] *Id.*

[23] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[24] *See* Jesse Damiani, *Your Social Security Number Costs $4 on the Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-securitynumber-costs-4-on-the-darkweb-new-report-finds/?sh=770cee3a13f1.

50. Social Security numbers—which, according to available information, were almost certainly compromised for approximately 25% of the Class members—are one of the most detrimental forms of Private Information to have stolen due to the multitude of fraudulent purposes for which they can be used and the significant challenge individuals face in changing them.

51. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases."[25] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[26]

52. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

53. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[27]

54. Theft of PHI, which, upon information and belief, was compromised in the Data Breach, is also gravely serious, putting patients at risk of medical identity theft wherein "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims

[25] *See Avoid Identity Theft: Protect Social Security Numbers,* Soc. Sec. Phila. Reg., https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases (last visited January 21, 2025).

[26] Id.

[27] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015, 4:59 AM), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[28]

55. A study conducted by Experian revealed that the average cost of medical identity theft per incident is approximately $20,000. Additionally, the majority of victims of medical identity theft are compelled to cover out-of-pocket expenses for healthcare services they did not receive in order to reinstate their coverage. Furthermore, almost half of medical identity theft victims lose their healthcare coverage following the incident, while nearly one-third experience an increase in insurance premiums. Alarmingly, 40 percent of victims are unable to fully resolve their identity theft ordeal.[29]

56. Moreover, fraudulent medical treatment can have non-financial impacts. Deborah Peel, executive director of Patient Privacy Rights, has described scenarios in which an individual may be given an improper blood type or administered medicines because their medical records contain information supplied by an individual obtaining treatment under a false name.[30]

57. Further, loss of personal health information, such as treatment history, diagnoses, and prescription information, exposes the victims to loss of reputation, loss of employment, blackmail, and other harms including the trauma of having your most personal details published online for all to see. This trauma is particularly acute for juvenile victims. Many of these kids now have to live, wondering if information about their home lives and medical histories will be disclosed and used against them.

58. PII also sells on legitimate markets, an industry that is valued at hundreds of billions of dollars per year. Customers themselves are able to sell non-public information directly to data

---

[28] *Medical I.D. Theft*, EFraudPrevention, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last visited January 21, 2025).

[29] *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, (March 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-themand-what-to-do-after-one/.

[30] *See 2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse*, WASH. POST, Andrea Peterson, Mar. 20, 2015, available at http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last visited Mar. 10, 2016).

brokers who aggregate the information for sale to marketers or others. Consumers may also sell their web browsing histories to the Nielson Corporation for up to $50 annually.

59. Because their Private Information has value, Plaintiff and Class members must take significant protective measures, including years of constant surveillance of their financial and personal records, credit monitoring, and identity protection.

PowerSchool Owed Duties to Safeguard Individuals' Private Information

60. Beyond the obligations arising from PowerSchool's own representations keeping Plaintiff's and Class Members' data secure, PowerSchool owed Plaintiff and Class members a duty to safeguard their Private Information.

61. As described further below, PowerSchool owed a duty to safeguard Private Information under several statutes, including the Federal Trade Commission Act ("FTC Act") and the Children's Online Privacy Protection Act ("COPPA"), to ensure that all information they maintained was secure. These statutes were enacted to protect Plaintiff and the Class members from the type of conduct in which PowerSchool engaged.

62. PowerSchool owed a duty to safeguard Private Information because they were on notice that they were handling highly valuable data and knew there was a risk it would be targeted by cybercriminals. Moreover, PowerSchool knew of the extensive, foreseeable harm that would ensue for the victims of a data breach and therefore owed a duty to safeguard that information.

63. Given the sensitive nature of the Private Information contained in PowerSchool's systems, PowerSchool knew that hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, socially-engineered attacks, healthcare fraud, and other identity-related fraud upon exfiltrating that data from PowerSchool's system. PowerSchool also knew that individuals whose Private Information was maintained in PowerSchool's system would reasonably spend time and effort to mitigate their damages and prevent identity theft and fraud, if that Private Information were taken.

64. PowerSchool also owed a duty to safeguard Plaintiff's and Class members' data based upon the promises that they made to their customers to securely store data. PowerSchool

voluntarily undertook efforts to keep that data secure in their business operations and thus owe a continuing obligation to Plaintiff and Class members to keep their Private Information secure.

65. The duty to protect Plaintiff's and Class members' Private Information is non-delegable. PowerSchool's business model is premised upon voluntarily assuming this duty, by soliciting customers to rely on its professed ability to store sensitive data securely. PowerSchool's duty is for the benefit of the individuals whose Private Information its products store and manage.

66. PowerSchool also owed a duty to comply with industry standards in safeguarding Private Information, which they did not do.

67. Because of the value of Private Information to hackers and identity thieves, companies in the business of storing, maintaining, or securing Private Information such as PowerSchool, have been identified as being particularly vulnerable to cyberattacks. Cybersecurity firms have promulgated a series of best practices that at minimum should be implemented by sector participants including: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; and training staff regarding critical points.

68. Federal and state government bodies have likewise established security standards and issued recommendations to reduce the risk of data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for business highlighting the importance of robust and effective data and cybersecurity practices. According to the FTC, the imperative of data and cybersecurity should be factored into all business decision-making.

69. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data and cybersecurity principles and practices for business. The guidelines note businesses should protect the personal customer and consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines further recommend that businesses

use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

70. The FTC also recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ appropriate measures to protect against unauthorized access to confidential consumer data as an unfair practice that violates Section 5 of the FTC Act, 15 U.S.C. § 45. Orders in these actions further clarify the measures businesses must take to meet their data and cybersecurity obligations.

72. Further, pursuant to COPPA, 15 U.S.C. § 312.10, PowerSchool had a "mandate[d]" duty to only "retain children's personal information 'for only as long as is reasonably necessary to fulfill the purpose for which the information was collected[,]'" and thereafter had a duty to "delete [children's personal information] using reasonable measures to ensure it's been securely destroyed" even absent a parent's request for the deletion of a child's personal information.

73. Data breaches can be prevented. Cybersecurity professionals and applicable information security standards urge organizations to take reasonable technical and administrative information security controls. Commonly recommended controls include: ensuring computer networks are adequately segmented, implementing and configuring intrusion prevention and detection technologies, monitoring computer systems using appropriate tools and responding to alerts on suspicious behavior, implementing spam and malware filters, requiring multifactor authentication for external access, implementing secure cryptographic algorithms, timely applying security patches and updates, limiting the use of privileged or administrative accounts, training employees on the handling of suspicious emails, implementing an effective vulnerability

management program, ensuring vendors implement and maintain adequate security controls, and implementing heightened security controls around sensitive data sources.

74. The Data Breach underscores PowerSchool's failure to sufficiently implement one or more vital security measures aimed at preventing cyberattacks. The Data Breach never would have occurred without PowerSchool's inadequate cybersecurity controls, enabling data thieves to access and acquire the Private Information of, according to available information, thousands to tens of thousands of individuals, including Plaintiff and Class members.

75. At all relevant times, PowerSchool knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class members and of the foreseeable consequences that would occur if PowerSchool's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members as a result of a breach.

76. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

The Data Breach Harmed Plaintiff and Class Members

77. As a result of PowerSchool's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the hands of criminals, the risk of identity theft to the Plaintiff and Class members has materialized and is imminent. Consequently, Plaintiff and Class members have sustained actual and imminent injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the effects of the Data Breach; (v) loss of benefit of the bargain; (vi) nominal damages; and (vii) the continued and increased risk to their Private Information, which remains inadequately secured and accessible to unauthorized third parties and is still stored in PowerSchool's systems, subject to further unauthorized disclosures unless PowerSchool implements appropriate and adequate protective measures.

78. The Private Information of Plaintiff and Class members will almost certainly end up being distributed through illicit underground criminal networks, including being sold on the dark web, as that is the modus operandi of hackers. Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class members. Simply put, unauthorized individuals could easily access the Private Information of Plaintiff and Class members.

79. As a result of the Data Breach, hackers can now commit identity theft, financial fraud, and other fraud against Plaintiff and Class members, given the stolen Private Information's sensitive nature. Plaintiff and Class members therefore have suffered injury and face an imminent, substantial risk of further injuries like identity theft and related cybercrimes.

80. The Private Information likely exposed in the Data Breach is highly valuable and sought after on illicit underground markets for use in committing identity theft and fraud. Malicious actors use this data to access bank accounts, credit cards, and social media accounts, among other things. They may also use the Private Information to open new financial or utility accounts, seek medical treatment using victims' insurance, file fraudulent tax returns, seek and obtain government benefits or government IDs, or create new identities for use in committing frauds. Because victims of breaches can become less diligent in account monitoring over time, bad actors may wait years before using the Private Information, or they may re-use it to commit several cybercrimes.

81. Even where individuals receive reimbursement for resulting financial losses, they are not made whole again because of the significant time and effort required to do so. The Government Accountability Office reported that criminals often hold onto stolen data for more than a year after it is obtained, waiting for victims to become less vigilant before using the data to commit identity theft. And fraudulent use of data may continue for years after its sale or

publication. The GAO concluded that studies that try to measure harms from data breaches "cannot necessarily rule out all future harm."[31]

82. The Identity Theft Resource Center's 2021 survey reported that victims of identity theft reported suffering negative experiences and emotional harms: anxiety (84%); feelings of violation (76%); rejection for credit or loans (83%); financial related identity problems (32%); resulting problems with family members (32%); feeling suicidal (10%).[32]

83. Physical harms also result from identity theft. A similar survey found that victims suffered resulting physical symptoms: sleep disturbances (48.3%); inability to concentrate / lack of focus (37.1%); inability to work because of physical symptoms (28.7%); new physical illnesses including stomach problems, pain, and heart palpitations (23.1%); starting or relapsing into unhealthy or addictive behaviors (12.6%).[33]

84. Theft of PHI carries significant consequences. A thief could potentially exploit identity or health insurance details to seek medical treatment, obtain prescription medications, submit claims to a data breach victim's insurance provider, or access other healthcare services. If the thief's health information becomes intertwined with data breach victim's, it could impact victim's medical treatment, insurance coverage, payment records, and even victim's credit report.

[31] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown*, U.S. GOV'T. ACCOUNTABILITY OFF., http://www.gao.gov/new.items/d07737.pdf (last visited January 21, 2025).

[32] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/wpcontent/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf.

[33] *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited January 21, 2025).

85. Unauthorized disclosure of sensitive Private Information also reduces its value to its rightful owner, as recognized by courts as an independent source of harm.[34] PII and PHI constitute valuable property rights.[35]

86. Even consumers who have been victims of previous data breaches are injured when their data is stolen and traded. Each data breach increases the likelihood that the victim's personal information will be exposed on the dark web to more individuals who are looking to misuse it.

87. Because of these injuries resulting from the Data Breach, Plaintiff and Class members suffer and continue to suffer economic loss and actual harm, including:

- disclosure or confidential information to a third party without consent;
- loss of the value of explicit and implicit promises of data security;
- identity fraud and theft;
- anxiety, loss of privacy, and emotional distress;
- the cost of detection and prevention measures for identity theft and unauthorized financial account use;
- lowered credit scores from credit inquiries;
- unauthorized charges;
- diminution of value of PII and PHI;
- loss of use of financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amounts they were permitted to obtain from accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- costs of credit monitoring, identity theft production services, and credit freezes;
- costs associated with loss of time or productivity or enjoyment of one's life from the time required to mitigate and address consequences and future consequences of the Data Breach, such as searching for fraudulent activity, imposing withdrawal and purchase limits, as well as the stress and nuisance of Data Breach repercussions;
- imminent, continued, and certainly impending injury flowing from the potential fraud and identity theft posed by the unauthorized possession of data by third parties.

[34] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

[35] U.S. GOV'T. ACCOUNTABILITY OFF., *supra* note 31.

88. Plaintiff and Class members place a significant value on data security. About half of consumers consider data security to be a main or important consideration in their purchasing decision and would be willing to pay more to work with those with better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[36]

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

89. Considering the nature of the targeted attack in this case, involving sophisticated criminal activity and the sensitive Private Information at stake, there is a high likelihood that entire datasets of stolen information have either been or will be circulated on the black market or dark web. Criminals intend to exploit this Private Information for identity theft crimes, such as opening bank accounts in victims' names for purchases or money laundering, filing fraudulent tax returns, securing loans or lines of credit, or submitting false unemployment claims.

90. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

91. Consequently, Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

92. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per individual. This is reasonable and necessary cost to monitor to protect Plaintiff and Class members from the risk of identity theft that arose from PowerSchool's Data Breach.

93. While PowerSchool claims that it will offer 2-years of credit monitoring to the Data Breach victims, this is an inadequate duration. PowerSchool has not yet revealed the details of the free credit monitoring it will offer, but the products typically offered in the wake of data breaches

[36] *Beyond the Bottom Line: The Real Cost of Data Breaches,* FIREEYE, p. 14, (May 2016), https://web.archive.org/web/20230628100935/https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf.

are narrow products that provide insufficient monitoring and security for victims. To make matters worse, the Data Breach victims would have to provide even more Private Information to PowerSchool's chosen vendor to use the credit monitoring solution. Data Breach victims may be understandably skeptical about further trusting PowerSchool with their data.

Allegations Relating to Plaintiff Gramelspacher

94. Plaintiff Evan Gramelspacher is student at Olentangy Liberty High School in the Olentangy Local School District. Olentangy Local School District uses PowerSchool SIS to conduct its operations.

95. As part of his schooling, Plaintiff Gramelspacher provided his sensitive Private Information to his school, which provided it to PowerSchool.

96. At all times, Plaintiff Gramelspacher expected this information to be kept confidential, and likewise, expected any Private Information generated by his school district and provided to PowerSchool would be kept confidential.

97. On January 10, 2025, Plaintiff Gramelspacher and his family received an email from his school district stating that PowerSchool had informed them on January 7 that the Plaintiff's school district had failed to prevent the Data Breach. The school's notice conveyed PowerSchool's representations that it had "taken appropriate steps to prevent the data of its more than 60 million students and staff from further unauthorized access or misuse."

98. As a result, Plaintiff Gramelspacher spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, monitoring his accounts and seeking legal counsel regarding Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

99. Plaintiff Gramelspacher has suffered actual injury in the form of damages to and diminution in the value of his Private Information, which was compromised as a result of the Data Breach.

100. Plaintiff Gramelspacher has suffered and continues to suffer lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has had anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his Private Information.

101. Plaintiff Gramelspacher has also suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties/criminals.

102. Plaintiff Gramelspacher has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in PowerSchool's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

103. Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiff proposes the following "Class" definition, subject to amendment as appropriate:

> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach that PowerSchool disclosed in or about January 2025 (the "Class").

104. Excluded from the Class are the following individuals and/or entities: PowerSchool and PowerSchool's parents, subsidiaries, affiliates, officers and directors, and any entity in which PowerSchool has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, members of their immediate families, and chambers staff.

105. Plaintiff reserves the right to amend the definitions of the Class or add additional Classes or Subclasses.

106. Numerosity: The individuals of the Class are so numerous that joinder of all patients is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of PowerSchool, upon information and belief, millions of individuals were impacted. The Class is identifiable within

PowerSchool's records, and these individuals will be identified when PowerSchool completes its full review of the files that were impacted.

107. Commonality: Common questions of law and fact exist as to all individuals of the Class and predominate over any questions affecting solely individual patients of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent PowerSchool had a duty to protect the Private Information of Plaintiff and Class members;

b. Whether PowerSchool had respective duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;

c. Whether PowerSchool had respective duties not to use the Private Information of Plaintiff and Class members for non-business purposes;

d. Whether PowerSchool failed to adequately safeguard the Private Information of Plaintiff and Class members;

e. Whether PowerSchool failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether PowerSchool adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Plaintiff and Class members are entitled to actual damages and/or nominal damages as a result of PowerSchool's wrongful conduct;

h. Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

108. Typicality: Plaintiff's claims are typical of those of the other patients of the Class because Plaintiff, like other Class members, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

109. Policies Generally Applicable to the Class: This class action is also appropriate for certification because PowerSchool acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. PowerSchool's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenges of these policies hinge on PowerSchool's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

110. Adequacy: Plaintiff will serve as a fair and effective representative for the Class members, possessing no conflicting interests that would hinder the protection of their rights. The relief sought by the Plaintiff aligns with the collective interests of the Class, without any adverse implications for its members. The infringements upon the Plaintiff's rights and the damages incurred are emblematic of those experienced by other Class members. Moreover, Plaintiff has engaged legal counsel adept in navigating intricate class action and data breach litigation, demonstrating a commitment to vigorously pursue this case.

111. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against a large corporation like PowerSchool. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

112. The nature of this action and the nature of laws available to Plaintiff and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class members for the wrongs alleged because PowerSchool would otherwise necessarily gain an unconscionable advantage in individual suits since they would be

able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

113. The litigation of the claims brought herein is manageable. PowerSchool's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

114. Adequate notice can be given to Class members directly using information maintained in PowerSchool's records.

115. Unless a Class-wide injunction is issued, PowerSchool may continue in its failure to properly secure the Private Information of Class members, PowerSchool may continue to refuse to provide proper notification to Class members regarding the Data Breach, and PowerSchool may continue to act unlawfully as set forth in this Complaint.

116. Further, PowerSchool has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

117. Similarly, specific issues outlined in Rule 42(d)(1) warrant certification as they entail distinct yet shared concerns pivotal to advancing the resolution of this case and the interests of all parties involved. These issues include, but are not confined to:

a. Whether PowerSchool failed to promptly notify both Plaintiff and the Class about the Data Breach;

b. Whether PowerSchool bore a legal responsibility to exercise due diligence in the acquisition, storage, and protection of Private Information belonging to Plaintiff and the Class;

c. Whether the security measures implemented by PowerSchool to safeguard their data systems aligned with industry best practices endorsed by data security experts;

d. Whether PowerSchool's omission of adequate protective security measures amounted to negligence;

e. Whether PowerSchool neglected to undertake commercially reasonable measures to secure Private Information; and

f. Whether adherence to data security recommendations outlined by the FTC, by HIPAA and those advocated by data security experts could have feasibly prevented the occurrence of the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

118. Plaintiff re-alleges and incorporates by reference every allegation in the preceding paragraphs as if fully set forth herein.

119. PowerSchool collected and stored Plaintiff's and Class members' Private Information, including names, phone numbers, email addresses, residential addresses, Social Security numbers, tax identification numbers, dates of birth, financial information, medication information, immunization records, disability information, health insurance information photo identification, and employment information.

120. PowerSchool owed Plaintiff and Class members a duty of reasonable care to preserve and protect the confidentiality of their Private Information that it collected. This duty included, among other obligations, maintaining and testing its security systems and networks, and the systems and networks of its vendors, as well as taking other reasonable security measures to safeguard and adequately secure the Private Information of Plaintiff and the Class from unauthorized access and use.

121. PowerSchool's duties also arise by operation of statute. Pursuant to the FTC Act, 15 U.S.C. § 45, PowerSchool had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

122. Plaintiff and Class members were the foreseeable victims of PowerSchool's inadequate and ineffectual cybersecurity systems and protocols. The natural and probable consequence of PowerSchool's failing to adequately secure its information networks was Plaintiff's and Class members' Private Information being hacked.

123. PowerSchool knew or should have known that Plaintiff's and Class members' Private Information was an attractive target for cyber thieves, particularly in light of data breaches experienced by other entities around the United States. Moreover, the harm to Plaintiff and Class members from exposure of their highly confidential Private Information was reasonably foreseeable to PowerSchool.

124. PowerSchool had the ability to sufficiently guard against data breaches by monitoring and testing its systems and implementing adequate measures to protect its systems, such as using attack surface software.

125. PowerSchool breached its duty to exercise reasonable care in protecting Plaintiff's and Class members' Private Information by failing to implement and maintain adequate security measures to safeguard Plaintiff's and Class members' Private Information, failing to monitor its systems to identify suspicious activity, and allowing unauthorized access to, and exfiltration of, Plaintiff's and Class members' confidential Private Information.

126. There is a close connection between PowerSchool's failure to employ reasonable security protections for its customers and end users' Private Information and the injuries suffered by Plaintiff and Class members. When individuals' sensitive Private Information is stolen, they face a heightened risk of identity theft and may need to: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit

inquiries and charges; (5) place and renew credit fraud alerts on a quarterly basis; (6) contest fraudulent charges and other forms of identity theft; (7) repair damage to credit and financial accounts; and (8) take other steps to protect themselves and attempt to avoid or recover from identity theft and fraud

127. PowerSchool was in a special relationship with Plaintiff and Class members with respect to the hacked information because the end and aim of PowerSchool's data security measures was to benefit Plaintiff and Class members by ensuring that their personal information would remain protected and secure. Only PowerSchool was in a position to ensure that its systems were sufficiently secure to protect Plaintiff's and Class members' personal and medical information. The harm to Plaintiff and Class members from their exposure was highly foreseeable to PowerSchool.

128. The policy of preventing future harm disfavors application of the economic loss rule, particularly given the sensitivity of the private information entrusted to PowerSchool. A high degree of opprobrium attaches to PowerSchool's failure to secure Plaintiff's and Class members' personal and extremely confidential facts. PowerSchool had an independent duty in tort to protect this information and thereby avoid reasonably foreseeable harm to Plaintiff and Class members.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Class)

129. Plaintiff re-alleges and incorporates by reference every allegation in the preceding paragraphs as if fully set forth herein.

130. According to the Federal Trade Commission Act, 15 U.S.C. § 45, PowerSchool was obligated to furnish fair and adequate computer systems and data security practices to protect the private information of both the Plaintiff and Class members.

131. PowerSchool breached its duties to Plaintiff and Class members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

132. Further, pursuant to COPPA, 15 U.S.C. § 312.10, PowerSchool had a "mandate[d]" duty to only "retain children's personal information 'for only as long as is reasonably necessary to fulfill the purpose for which the information was collected[,]'" and thereafter had a duty to "delete [children's personal information] using reasonable measures to ensure it's been securely destroyed" even absent a parent's request for the deletion of a child's personal information.

133. PowerSchool violated COPPA § 312.10 by failing to use reasonable measures to protect PII and PHI and not complying with industry standards.

134. PowerSchool's failure to comply with applicable laws and regulations constitutes negligence per se.

135. Plaintiff and Class members are within the class of persons the statutes were intended to protect and the harm to Plaintiff and Class members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

136. But for PowerSchool's wrongful and negligent breach of their duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

137. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of PowerSchool's breach of their duties. PowerSchool knew or should have known that by failing to meet its duties, PowerSchool's breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

138. As a direct and proximate result of PowerSchool's negligent conduct, Plaintiff and Class members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III

Breach of Third-Party Beneficiary Contract

(On Behalf of Plaintiff and the Class)

139. Plaintiff re-alleges and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

140. PowerSchool contracted with Plaintiff's and the Class members' educational institutions for the provision of education software, which included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

141. Indeed, because such safeguards are required by industry standard and applicable statutory, common, and regulatory law, the implementation and maintenance of such safeguards is required to fulfill a PowerSchool's contractual obligations of good faith and fair dealing in their performance.

142. Such contracts were expressly made for the benefit of students, parents, and teachers, such as Plaintiff and the Class members, who gave their Private Information to their educational institutions and/or to PowerSchool as part of their schooling, the schooling of their children, or their employment at an educational institution.

143. PowerSchool advertised PowerSchool SIS as being a secure place to store and keep student data, claiming to their customers that "[w]e are dedicated to protecting your students' data with a comprehensive security program that starts with 'secure by design' principles at the inception of our products and extends through third-party penetration testing, robust cloud security, and a fully staffed 24x7x365 Security Operations Center." [37]

144. The benefit of collection, protection, and storage of Private Information was thus the direct, intended, and primary objective of the contracting parties as it related to those express terms.

145. PowerSchool breached its contract with each educational institution when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of the Plaintiff's and Class members' Private Information.

146. PowerSchool knew that if it breached such contracts, harm would befall its customers' students, parents, and teachers, including the Plaintiffs and the Class Members.

[37] *How PowerSchool Protects Data*, POWERSCHOOL, https://www.powerschool.com/studentinformation-cloud/powerschool-sis/ (last visited January 21, 2024).

147. As such, the PowerSchool's failure to uphold the terms of its contract and allow for the Data Breach has foreseeably harmed Plaintiff and Class members.

148. As a direct and proximate result of PowerSchool's breach, Plaintiff and Class members sustained damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in PowerSchool's possession and is subject to further unauthorized disclosures so long as PowerSchool fails to undertake appropriate and adequate measures to protect the Private Information.

149. Accordingly, Plaintiff and Class members are entitled to damages in an amount to be determined at trial, along with their costs, including attorneys' fees incurred.

150. Plaintiff and the Class are also entitled to injunctive relief requiring the PowerSchool to: (i) Strengthen its data security systems and monitoring procedures; (ii) Undergo annual audits of these systems and procedures in the future; and (iii) Immediately provide adequate credit monitoring to all Class members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representative, and Plaintiff's counsel as Class Counsel;

B. That the Court grant equitable relief enjoining PowerSchool from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class members;

C. That the Court grant injunctive relief requested by Plaintiff, including injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including an order:

i. requiring PowerSchool to conduct regular database scanning and securing checks;

ii. requiring PowerSchool to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class members;

iii. requiring PowerSchool to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with PowerSchool's policies, programs, and systems for protecting personal identifying information;

iv. requiring PowerSchool to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor PowerSchool's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

v. requiring PowerSchool to implement logging and monitoring programs sufficient to track traffic to and from PowerSchool's servers; and

vi. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate PowerSchool's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class,

and to report any deficiencies with compliance of the Court's final judgment;

D. That the Court award Plaintiff and Class members damages, including actual, nominal, consequential, and punitive damages, for each cause of action as allowed by law in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by PowerSchool as a result of its unlawful acts, omissions, and practices;

F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorney's fees, costs, and expenses;

G. That the Court award pre-and post-judgment interest at the maximum legal rate; and

H. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims so triable.

Date: January 22, 2025

Respectfully submitted,

/s/ David M. Berger

David Berger (State Bar No. 277526)
Jane Farrell (State Bar No. 333779)
Sarah E. Hillier (*pro hac vice* forthcoming)
Jennifer Sun (State Bar No. 354276)
GIBBS LAW GROUP LLP
1111 Broadway, Ste. 2100
Oakland, CA 94607
Tel: 510-350-9700
dmb@classlawgroup.com
mht@classlawgroup.com
jgf@classlawgroup.com
seh@classlawgroup.com
jsun@classlawgroup.com

Mark H. Troutman (*pro hac vice* forthcoming)
GIBBS LAW GROUP LLP
1554 Polaris Parkway, Suite 325
Columbus, Ohio 43240
Telephone: (510) 350-9700
Fax: (510) 350-9701
mht@classlawgroup.com

Counsel for Plaintiff and the Proposed Class